UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/769,173	01/30/2004	Sherman (Xuemin) Chen	15415US01	7811

23446 7590 05/09/2008
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
PALIWAL, YOGESH	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
05/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/769,173	CHEN ET AL.	
	Examiner	Art Unit	
	YOGESH PALIWAL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's amendment filed on Feb 14, 2008 has been entered. Currently claims 1-41 are pending in this application. Any well known art statements made in the prior office action not argued by applicant is taken as admittance of prior art as per MPEP 2144.03.

Response to Arguments

1. Applicant's arguments filed on Feb 14, 2008 have been fully considered but they are not persuasive for following reasons:

- Applicant argues: "The Applicant points out that the relevant claim limitation from Applicant's clam 1 is "encrypting the digitally signed secure key utilizing at least a previously generated unreadable digitally signed encrypted key". In other words, **a digitally signed secure key is encrypted by utilizing a digitally signed encrypted key that has been previously generated and it is unreadable.** The Examiner relies on Ellison for support and is apparently equating the session key Kx of Ellison to Applicant's "secure key". Ellison further discloses that the session key Kx is signed by a private key of the server and then **encrypted by the public key of the user Ple**. In other words, Ellison encrypts the signed secure key by simply using a public key. The Applicant points out that it is well known in the art of asymmetric cryptography, that the public key is widely distributed. In this regard, **the public key of the user Ple is not "unreadable"**, as recited in Applicant's claim 1. Furthermore, **the public key disclosed by Ellison is also not a digitally signed and encrypted key that has been previously generated**. Therefore, the Applicant maintains that the combination of Akiyama and Ellison does not disclose or

suggest at least the limitation of "encrypting the digitally signed secure key utilizing at least a previously generated unreadable digitally signed encrypted key," as recited by the Applicant in independent claim 1.

- In reply, Examiner is not sure as to how this argument is relevant to the rejection. Contrary to applicant's assertion, examiner is not equating the session key Kx of Ellison to Applicant's secure key. Examiner is equating the session key Kx of Ellison to the claimed master key that is digitally signed and encrypted. Examiner would like to point out that Akiyama discloses encrypting the digitally signed secure key utilizing at least a previously generated unreadable key (Fig. 7, "Enciphered contract information", also at Paragraph 0106, lines 5-8, "The individual control packet is comprised of an information identifier, master key identifier, and encrypted contract information, as shown in FIG. 7.", Note: [Each digitally signed contract information is encrypted using and master key, also note that master keys are generated and sent to clients via secure card therefore master keys are generated prior to encrypting work keys and it is also unreadable because only broadcaster and receivers have the master key (see Paragraph 0154)]. Therefore, Akiyama is only missing the claimed limitation that required that master key is also encrypted and digitally signed. Ellison reference is only used to teach encrypting and digitally signing a key.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Akiyama (US 2002/0001386) in view of Ellison (US 6,073,237), hereinafter Ellison.

Regarding **Claim 1**, Akiyama discloses a method for secure key authentication, the method comprising:

generating at a first location (Fig.29, This is a broadcast station where the contents, keys and digital signature for contact information etc, are generated and then sent to receivers) a digital signature (Fig. 5, "Digital signature") of a secure key to obtain a digitally signed secure key (Fig. 5, "work keys", also at paragraph 0107, "The digital signature is information used to check the authenticity of the contract information, and is used to prevent tampering.", also at paragraph 0107, "The contract information is made up of, e.g., a receiver ID, channel contract information, the number n of work keys, n pairs of work keys and work key identifiers, and digital signature").

encrypting the digitally signed secure key utilizing at least a previously generated unreadable key (Fig. 7, "Enciphered contract information", also at Paragraph 0106, lines 5-8, "The individual control packet is comprised of an information identifier, master key identifier, and encrypted contract information, as shown in FIG. 7.", Note: *[Each digitally signed contract information is encrypted using and master key, also note that master keys are generated and sent to clients via secure card therefore master keys are generated prior to encrypting work keys and it is also unreadable because only broadcaster and receivers have the master key (see Paragraph 0154)]*

and transmitting the digitally signed and encrypted secure key from the first location (Paragraph 0167, "The transmission processing operation of an individual control packet by the information distributor apparatus shown in FIG. 29..."). Note: individual control packets contains encrypted contract information (Paragraph 0106, "The individual control packet is comprised of an

information identifier, master key identifier, and encrypted contract information, as shown in FIG. 7."), and as established above, contract information contains work keys, as a result, when control packet is transmitted, it contains the signed work keys as well, and thus we can interpret that signed work keys are transmitted from a broadcast device depicted in Fig. 29).

Akiyama discloses encrypting work keys with master key. Akiyama does not disclose that the master key is also encrypted and digitally signed as now required by claim limitation.

However, using PKI system to encrypt and digitally signing the keys are well known technique in the art of cryptography, which enable secure transmission of keys over unsecured channels using asymmetric key encryption. Ellison, in the same field of endeavor of network security, discloses encrypting and digitally signing a key (Column 4, lines 64-67, "The session key K_x is signed by private key of the server itself K_n 121 and encrypted by the public key of the user P1e. The encrypted and signed session key K_x is then sent back to the user 123).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to add, on the master key of Akiyama, a digital signature utilizing a private key of a broadcast station and then encrypt the digitally signed key with the public key of the receiver, as taught by Ellison. One of ordinary skill in the art would be motivated to do so because digital signature provides authentication and encryption provides secrecy. As a result, when the broadcast station updates the master key, it could utilize PKI technique to send new master key over an unsecured channel with fully confidentiality without having to provide each receiver a new smart card having a new master key.

Regarding **Claim 2**, the rejection of claim 1 is incorporated and further Akiyama discloses generating the digital signature from at least one of an asymmetric encryption algorithm and a

symmetric encryption algorithm (Paragraph 0111, lines 9-10, "authenticates the digital signature using key information (secret key or public key) stored in a digital signature")

Regarding **Claim 3**, the rejection of claim 1 is incorporated and the combination of Akiyama and Ellison discloses encrypting the digitally signed secure key prior to transmission utilizing at least an encrypted master key, to obtain the digitally signed and encrypted secure key (Fig. 7, "Enciphered contract information", also at Paragraph 0106, lines 5-8, "The individual control packet is comprised of an information identifier, master key identifier, and encrypted contract information, as shown in FIG. 7.") *[Each digitally signed contract information is encrypted using and master key, and Ellison discloses, as established in the rejection of claim 1 above, the limitation of encrypting a master key]*

Regarding **Claim 4**, the rejection of claim 3 is incorporated and further Akiyama discloses the secure key comprises at least one of a master key, a work key and a scrambling key. (*Fig. 5, "Work keys")*

Regarding **Claim 5**, the rejection of claim 4 is incorporated and further Akiyama discloses the receiving the digitally signed and encrypted secure key at a second location **(Paragraph 0110, lines 1-2, "Upon receiving an individual packet via the public telephone network and modem 101...")**

decrypting the digitally signed and encrypted secure key to obtain a decrypted digitally signed secure key (Paragraph 0110, Lines 11-17, "If the master key identifier matches the master key, that master key is output from the master key storage 103 (step S4) to decrypt contract information in the individual information packet")

Regarding **Claim 6**, the rejection of claim 5 is incorporated and further Akiyama discloses if the secure key comprises a work key then a decrypted digitally signed master key at the second location

is utilized for decrypting an encrypted digitally signed work key (Paragraph 0110, Lines 11-17, "If the master key identifier matches the master key, that master key is output from the master key storage 103 (step S4) to decrypt contract information in the individual information packet (step S5). Work key information (pairs of work key identifiers and work keys and the like) contained in the decrypted contract information is stored in a work key storage 105")

Regarding **Claim 7**, the rejection of claim 5 is incorporated and further Akiyama discloses if the secure key comprises a scrambling key then a decrypted digitally signed work key at the second location is utilized for decrypting an encrypted digitally signed scrambling key (Paragraph 0125, lines 9-14, "If the work key can be acquired, information of an encrypted section in the common control packet is decrypted using the work key (step S44). A channel key Kch is acquired from the decrypted information, and is stored in the channel key storage 118")

Regarding **Claim 8**, the rejection of claim 5 is incorporated and further Akiyama discloses verifying authenticity of the digital signature of the digitally signed secure key (Paragraph 0112, line 1-2, "digital signature authentication process")

Regarding **Claim 9**, the rejection of claim 8 is incorporated and further Akiyama discloses verifying the authenticity of the digital signature utilizing at least one of an asymmetric decryption algorithm and a symmetric decryption algorithm (Paragraph 0111, lines 7-11, "the contract information certifying device 107 certifies or authenticates the digital signature using key information (secret key or public key) stored in a digital signature authentication key storage 108")

Regarding **Claim 10**, the rejection of claim 8 is incorporated and further Akiyama discloses determining whether to verify authenticity of the digital signature (Paragraph 0111, lines 6-8, "If the

two IDs match, the contract information certifying device 107 certifies or authenticates the digital signature using key information")

Claims **11, 21 and 32** are "computer program" and "system" claims analogous to "method" claim 1. Akiyama in the same reference discloses a system for performing method of claim 1 [Broadcast receiver is depicted in figure 1 and Transmitter system is depicted in figure 29]. Also, it should be noted that since Akiyama's system discloses the hardware to perform the method of claim 1, therefore it would also have computer software that performs the method of claim 1. Claims 11, 21 and 32 are rejected under same rationale as the rejection of claim 1.

Claims **12, 22 and 33** are "computer program" and "system" claims analogous to "method" claim 2. Claims 12, 22 and 32 are rejected under same rationale as the rejection of claim 2.

Claims **13, 23 and 34** are "computer program" and "system" claims analogous to "method" claim 3. Claims 13, 23 and 34 are rejected under same rationale as the rejection of claim 3.

Claims **14, 24 and 35** are "computer program" and "system" claims analogous to "method" claim 4. Claims 14, 24 and 35 are rejected under same rationale as the rejection of claim 4.

Claims **15, 25 and 36** are "computer program" and "system" claims analogous to "method" claim 5. Claims 15, 25 and 36 are rejected under same rationale as the rejection of claim 5.

Claims **16, 26 and 37** are "computer program" and "system" claims analogous to "method" claim 6. Claims 16, 26 and 37 are rejected under same rationale as the rejection of claim 6.

Claims **17, 28 and 38** are "computer program" and "system" claims analogous to "method" claim 7. Claims 17, 28 and 38 are rejected under same rationale as the rejection of claim 7.

Claims **18, 28 and 39** are "computer program" and "system" claims analogous to "method" claim 8. Claims 18, 28 and 39 are rejected under same rationale as the rejection of claim 8.

Claims **19, 29 and 40** are "computer program" and "system" claims analogous to "method" claim 9. Claims 19, 29 and 40 are rejected under same rationale as the rejection of claim 9.

Claims **20, 30 and 41** are "computer program" and "system" claims analogous to "method" claim 10. Claims 20, 30 and 41 are rejected under same rationale as the rejection of claim 10.

Regarding **Claim 31**, rejection of claim 21 is incorporated and further Akiyama discloses at least one processor comprises at least one of a host processor, a microprocessor, and a microcontroller (Figure 29, processor used in the system of Fig. 29 is a host processor).

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2135

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135